REMARKS

The Examiner is thanked for the performance of a thorough search.

SPECIFICATION

In the specification, the paragraph on page 5, line 21 through page 6, line 1 has been amended to correct a typographical error. No new matter is introduced.

The paragraph on page 6, line 16 through page 7, line 6 has been amended to add the serial number of the co-pending application and to correct the title of same. No new matter is introduced.

The paragraph on page 24, line 21 through page 25, line 8 has been amended to add the serial numbers and filing dates of the two co-pending applications. No new matter is introduced.

STATUS OF CLAIMS

Claims 1-5, 8-15, 18-24, 26-28, and 31 have been amended.

Claims 32-80 have been added.

No claims have been cancelled or withdrawn.

Claims 1-80 are currently pending in the application.

SUMMARY OF THE REJECTIONS

Claims 1-31 have been rejected under 35 U.S.C. § 102b) as allegedly anticipated by U.S. Patent Number 5,748,736 issued to Mittra (" *Mittra*"). The rejections are respectfully traversed.

A. CLAIM 1

(1) INTRODUCTION TO CLAIM 1

Claim 1 features:

"A method for managing addition and deletion of network nodes from and to a secure multicast or broadcast group of network nodes in a communications network without a single point of failure, wherein each of the network nodes is associated with one of a ***plurality of group controllers***, wherein each group controller of the ***plurality of group controllers*** is a replica of a particular

group controller, and wherein the network nodes and the ***plurality of group controllers*** are logically organized in a **binary tree** that represents the network nodes and the ***plurality of group controllers***, in which leaf nodes of the **binary tree** represent network nodes that are joining or leaving the secure multicast or broadcast group, intermediate nodes represent other network nodes, and *root nodes* represent the ***plurality of group controllers***, the method comprising the steps of:

joining a first group controller to the ***plurality of group controllers*** in a local network;

establishing a secure communication channel between the first group controller and a second group controller of the ***plurality of group controllers*** using a key exchange protocol;

receiving a request to add or delete a network node of the secure multicast or broadcast group from a **load balancer** that is coupled to the ***plurality of group controllers***;

creating and storing a new group session key for each network node represented in each branch of the **binary tree** that is affected by adding or deleting the network node from the secure multicast or broadcast group;

distributing a group session key from a third group controller of the ***plurality of group controllers*** to the network nodes." (Emphasis added.)

Thus, Claim 1 features an approach for managing the addition and deletion of network nodes for a secure multicast or broadcast group without a single point of failure that includes the following features: (a) a ***plurality of group controllers***; (b) each group controller of the ***plurality of group controllers*** is a **replica** of a particular group controller; (c) a **binary tree**; (d) *root nodes* of the binary tree that represent the plurality of group controllers; and (e) a **load balancer** that is coupled to the ***plurality of group controllers***.

Note that in Claim 1, a plurality of group controllers is featured, which by definition means two or more group controllers, and each group controller in the plurality of group controllers is a replica of a particular group controller. The use of a plurality of group controllers, instead of a single group controller, addresses the drawback of a single group controller being a potential bottleneck (see Application, page 6, lines 9-11) and the issue that a central group controller presents a single point of failure (see Application, page 7, lines 7-9).

Also note that, by definition, in a binary tree, each node contains one parent node and no more than two child nodes, as exemplified in the embodiment illustrated in FIG. 5 of the Application.

(2) DISCUSSION OF *MITTRA*

In contrast to the approach of Claim 1, *Mittra* discloses an approach for secure group communication via a multicast or broadcast transmission that uses a group security controller (GSC) and at least one trusted intermediary (TI) server. In particular, *Mittra* notes that the "inventive 'secure multicast' implement by the FIG. 1 system is controlled by a ***single*** group security controller (GSC 111), and the inventive 'secure multicast' group implemented by each of the systems of FIGS. 2 and 3 is controlled by a ***single*** group security controller (GSC 11 or 211)." (Col. 6, lines 62-67; emphasis added.)

Note that the approach of *Mittra* is vulnerable to the single point of failure problem due to the use of just a single group security controller. Also note that while *Mittra* is described in terms of a secure multicast group having a hierarchical structure (Col. 7, line 1; Figures 1-3), the ***hierarchical structure is not in the form of a binary tree*** because many nodes have more than two child nodes (e.g., in Figure 1, multicast/unicast network 112A has six child nodes and multicast/unicast networks 112B and 112D each have three child nodes; Figures 2 and 3 include corresponding examples of three or more child nodes).

(3) THE OFFICE ACTION'S CITATIONS FROM *MITTRA*

The Office Action states that *Mittra* discloses Claim 1, citing "Fig. 1-3" with respect to the preamble of Claim 1 and "col. 7 line 25 to col 8 line 65" with respect to the five steps of Claim 1. For this issue and many other issues, the Office Action does not specify exactly what in *Mittra* corresponds to or constitutes each element or feature of the claims. In an Office Action "the particular part relied on must be designated as nearly as practicable ... The pertinence of each reference, if not apparent, must be clearly explained ..." (MPEP §707, citing 37 C.F.R. §1.104(c)(2)), and "the particular figure(s) of the drawings(s), and/or page(s) or paragraph(s) of the reference(s), and/or any relevant comments briefly stated should be included." (MPEP §707). The present citations to the references do not provide the Applicant with adequate notice or reasonable particularity with respect to the basis of the rejections. Instead, large portions of the references are simply identified in a non-specific way.

Specifically, in the rejection of Claim 1, all the figures of *Mittra* along with over a column and a half of the description of *Mittra* are cited in bulk after a recitation of the contents of Claim 1. As a result, the Applicant have had to engage in guesswork to determine the basis of the rejection. The Applicant cannot see any structure or functions in *Mittra* that correspond to the claims. As best understood by the Applicant, the rationale of the Office Action is technically incorrect in the rejection of Claim 1, as explained below.

(a) "Plurality of Group Controllers"

The approach of Claim 1 involves a "***plurality of group controllers***," yet *Mittra* only discloses the use of one group security controller (GSC), and *Mittra* emphasizes with respect to Figures 1-3, that only a "single" group security controller is used. (Col. 6, lines 62-67.) All of Figures 1-3 in *Mittra* disclose only one GSC (e.g., GSC 11 in Figure 1, GSC 11 in Figure 2, and Sender/GSC 211 in Figure 3).

Mittra explains that "all that is required to begin secure multicast is that the GSC is started up. Once this is done, senders and receivers apply to join the group as described below." (Col. 7, lines 32-34; emphasis added). "Joining a secure multicast group requires the joining member first to set up a separate secure channel with the GSC of the group (using a unicast communication line)." (Col. 7, lines 45-47; emphasis added). "Only the GSC maintains information concerning group membership; members do not know about each other..." (Col. 7, lines 64-65; emphasis added). *Mittra* then describes the set up of the secure channel (Col. 8, lines 3-14), then the communications between the GSC and the new member (Col. 8, lines 15-22), the communication of the new Kgrp to the multicast and the new member (Col. 8, lines 23-35), and then two cases for handling a member leaving the group (Col. 8, lines 36-67). Thus, the cited portion of the description of *Mittra* fails to disclose anything other than a single group security controller.

In the rejections of Claims 11 and 31 that include the same steps as in Claim 1, the Office Action also cites "col. 6 line 4 to col. 7 line 15 and col. 13 line 57 to col. 14 line 10." Yet as with the first cited portion from *Mittra* above used in the rejection of Claim 1 as well as Claims 11 and 13, these additional cited portions fail to disclose anything about a "plurality of group controllers" as featured in Claim 1. In particular, *Mittra* describes Figures 1, 2, and 3 (Col. 6, lines 4-44), which are addressed above, and then *Mittra* describes the types of devices in which the techniques of *Mittra* can be used, noting that a "single group security

controller" controls the groups implemented as illustrated in Figures 1, 2, and 3. (Col. 6, lines 45-67; emphasis added.) Then *Mittra* explains that each secure multicast group has subgroups that are served by different TI servers. (Col. 7, lines 1-15.) In addition, *Mittra* describes a member leaving a secure multicast group using trusted intermediaries (Col. 13, lines 57-67) and sending multicast transmissions with trusted intermediaries (Col. 14, lines 1-10.) However, nothing in these cited portions of Mittra disclose a "plurality of group controllers" as featured in Claim 1.

Therefore, the Applicant respectfully submits that *Mittra* does not disclose, teach, suggest, or in any way render obvious a "***plurality of group controllers***" as featured in Claim 1.

(b) "Replica of a Particular Group Controller"

Claim 1 also features that "each group controller of the ***plurality of group controllers*** is a replica of a particular group controller." As described in the Application, a "plurality of replicated group controllers GC, GC1, GC2, GC3, GC *N* are communicatively coupled. Any number of group controllers may be joined in such a network, as indicated by the designation GC *N*. A load balancer 1002 controls direction of communication requests to the group controllers. ***Each group controller*** GC, GC1, etc., is a replica of a ***group controller*** of the type shown in FIG. 6B and exemplified by group controller 501. Thus, each group controller GC, GC1, etc. manages a plurality of nodes arranged in a binary tree, such as binary tree 500 associated with group controller 501." (Page 37, line 19 through page 38, line 3; emphasis added.)

In other words, the approach of Claim 1 addresses the problems discussed above from the Background section of the Application of how the use of only a single group controller creates a bottleneck and presents a single point of failure. By using a plurality of group controllers, each of which is a replica of a particular group controller, the failure of a single group controller does not disrupt the multicast or broadcast group since there is at least one other group controller that can handle the functions of the failed group controller. Furthermore, the use of the plurality of group controllers, along with a load balancer to distribute processing among the plurality of group controllers, minimizes a single group controller serving as a bottleneck.

In contrast to Claim 1, *Mittra* fails to disclose anything related to a group controller being a replica of another group controller. In fact, an electronic search of *Mittra* reveals that the word "replica" is not even included in *Mittra*. And as discussed above, since *Mittra* fails to disclose a plurality of group controllers, *Mittra* also fails to disclose a plurality of group controllers that are replicas of a particular group controller.

Therefore, the Applicant respectfully submits that *Mittra* does not disclose, teach, suggest, or in any way render obvious "each group controller of the ***plurality of group controllers*** is a **replica** of a particular group controller" as featured in Claim 1.

(c) "Binary Tree"

Claim 1 also features a "**binary tree**" that includes several different types of nodes, such as leaf nodes representing the network nodes that are joining or leaving the group, intermediate nodes representing other network nodes, and root nodes representing the plurality of group controllers. As discussed above, the reason why a "binary tree" is so named is because each node in the binary tree has one parent node and no more than two child nodes. Thus, at each node of the binary tree, there are at most two branches (hence, "binary") leading to child nodes (see Application, FIG. 5).

The Applicant cannot identify anything in the portion of *Mittra* cited in the Office Action in the rejection of Claim 1 that remotely resembles any kind of hierarchical structure or tree, little less a binary tree as featured in Claim 1. In fact, an electronic search of *Mittra* reveals that the word "binary" is not even included in *Mittra*. However, other portions of *Mittra* disclose that the "TI [trusted intermediary] servers create a (logical) hierarchy of secure multicast networks (the secure distribution tree)..." (Col. 4, lines 21-23) and that the "secure multicast group has a hierarchical structure." (Col. 7, line 1.)

Nevertheless, the tree-based hierarchy described in *Mittra* is not a "binary" tree as featured in Claim 1. In each of Figures 1, 2, and 3 of *Mittra*, several nodes have three or more child nodes and thus cannot be a binary tree. Specifically, in Figure 1: multicast/unicast network 112A has six child nodes, namely sender 113A, receivers 114A, 114B, and TI 115A, 115B, 115C; multicast/unicast network 112B has three child nodes, namely receiver 114C and senders 113B, 113C; and multicast/unicast network 112D has three child nodes, namely receivers 114D, 114E, 114F. Multicast/unicast network 12A, 12B, 12D of Figures 2 and 3 are similar.

Therefore, the Applicant respectfully submits that *Mittra* does not disclose, teach, suggest, or in any way render obvious a "**binary tree**" as featured in Claim 1.

(d) "Root Nodes of the Binary Tree that Represent the Plurality of Group Controllers"

Claim 1 also features that "*root nodes* of the binary tree that represent the ***plurality of group controllers***." Again, the Applicant cannot identify anything in the cited portion of *Mittra* or elsewhere that corresponds to root nodes representing a plurality of group controllers. In fact, an electronic search of *Mittra* reveals that the word "root" is not even included in *Mittra*. Even if in Figures 1-3 of *Mittra* the topmost node is assumed to be a root node, the topmost node only corresponds to the single group security controller, not a plurality of group controllers and little less the root node of a binary tree, as featured in Claim 1.

Therefore, the Applicant respectfully submits that *Mittra* does not disclose, teach, suggest, or in any way render obvious "*root nodes* of the binary tree that represent the plurality of group controllers" as featured in Claim 1.

(e) "Load Balancer"

Claim 1 also features a "**load balancer** that is coupled to the ***plurality of group controllers***." Once again, the Applicant cannot identify anything in the cited portion of *Mittra* or elsewhere that corresponds to a load balancer, little less a load balancer coupled to a plurality of group controllers. In fact, an electronic search of *Mittra* reveals that neither the word "load" nor the word "balancer" are even included in *Mittra*. The cited portion of *Mittra* makes clear that there is only a single group security controller, and thus there is no set of two or more devices among which a load can be distributed, such as by a load balancer.

In the rejection of Claim 24, which includes the step of "load balancing traffic emanating from a plurality of network nodes to the plurality of group controllers," the Office Action cites "col. 9 line 48 to line 62." Yet again, the cited portion of *Mittra* fails to disclose anything related to load balancing or a load balancer. Rather, the cited portion of *Mittra* is the introductory paragraphs in the "Sending Multicast Transmissions" and describes several message digests and other means of encryption (Col. 9, lines 48-62), yet this discussion is in no way related to a load balancer or load balancing, as featured in either Claim 1 or Claim 24.

Therefore, the Applicant respectfully submits that *Mittra* does not disclose, teach, suggest, or in any way render obvious a "**load balancer** that is coupled to the ***plurality of group controllers***" as featured in Claim 1.

(4) CONCLUSION OF DISCUSSION OF CLAIM 1 AND *MITTRA*

Because *Mittra* fails to disclose, teach, suggest, or in any way render obvious (a) "a ***plurality of group controllers***"; (b) "each group controller of the ***plurality of group controllers*** is a **replica** of a particular group controller;" (c) a "**binary tree**;" (d) "*root nodes* of the binary tree that represent the plurality of group controllers;" and (e) "a **load balancer** that is coupled to the ***plurality of group controllers***," the Applicant respectfully submits that, for at least the reasons stated above, Claim 1 is allowable over the art of record and is in condition for allowance.

B. CLAIMS 11, 31, AND 41

Claims 11, 31, and 41 contain features that are that same as those described above with respect to Claim 1. Specifically, Claims 11, 31, and 41 all feature (a) "a ***plurality of group controllers***," (b) "each group controller of the ***plurality of group controllers*** is a **replica** of a particular group controller," (c) a "**binary tree**," (d) "*root nodes* of the binary tree that represent the plurality of group controllers," and (e) "a **load balancer** that is coupled to the ***plurality of group controllers***," as in Claim 1. Therefore, based on at least the reasons stated above with respect to Claim 1, the Applicant respectfully submits that Claims 11, 31, and 41 are allowable over the art of record and are in condition for allowance.

C. CLAIMS 21, 24, 51, 54, 61, 64, 71, AND 74

Claims 21, 24, 51, 54, 61, 64, 71, and 74 contain features that are either the same as or similar to those described above with respect to Claim 1. Specifically, Claims 21, 51, 61, and 71 all feature "a ***plurality of group controllers***", a "**binary tree**," and "*root nodes* of the binary tree that represent the plurality of group controllers," which are the same as in Claim 1, and "a first group controller comprising information that is replicated in a plurality of group controllers" and "a load balancer that controls distribution of requests to the plurality of group controllers," which are similar to the corresponding features of Claim 1. Also, Claims 24, 54, 64, and 74 all feature (a) "a ***plurality of group controllers***" and (b) a "**binary tree**," which

are the same as in Claim 1, and "load balancing traffic emanating from a plurality of network nodes to the plurality of group controllers" and "the plurality of group controllers correspond to the root node," which are similar to the corresponding features of Claim 1.

Therefore, based on at least the reasons stated above with respect to Claim 1, the Applicant respectfully submits that Claims 21, 24, 51, 54, 61, 64, 71, and 74 are allowable over the art of record and are in condition for allowance.

D. CLAIMS 2-10, 12-20, 22-23, 25-30, 32-40, 42-50, 52-53, 55-60, 62-63, 65-70, 72-73, AND 75-80

Claims 2-10, 12-20, 22-23, 25-30, 32-40, 42-50, 52-53, 55-60, 62-63, 65-70, 72-73, and 75-80 are dependent upon Claims 1, 11, 21, 24, 31, 41, 51, 54, 61, 64, 71, and 74 respectively, and thus include each and every feature of the corresponding independent claims. Each of Claims 2-10, 12-20, 22-23, 25-30, 32-40, 42-50, 52-53, 55-60, 62-63, 65-70, 72-73, and 75-80 is therefore allowable for the reasons given above for the Claims 1, 11, 21, 24, 31, 41, 51, 54, 61, 64, 71, and 74. In addition, each of Claims 2-10, 12-20, 22-23, 25-30, 32-40, 42-50, 52-53, 55-60, 62-63, 65-70, 72-73, and 75-80 introduces one or more additional limitations that independently render it patentable. However, due to the fundamental differences already identified, to expedite the positive resolution of this case a separate discussion of those limitations is not included at this time. Therefore, it is respectfully submitted that Claims 2-10, 12-20, 22-23, 25-30, 32-40, 42-50, 52-53, 55-60, 62-63, 65-70, 72-73, and 75-80 are allowable for the reasons given above with respect to Claims 1, 11, 21, 24, 31, 41, 51, 54, 61, 64, 71, and 74.

CONCLUSION

The Applicant believes that all issues raised in the Office Action have been addressed and that allowance of the pending claims is appropriate. After entry of the amendments, further examination on the merits is respectfully requested.

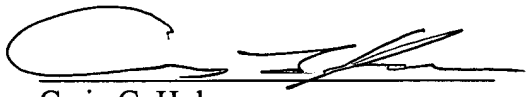
The Examiner is respectfully requested to contact the undersigned by telephone if it is believed that such contact would further the examination of the present application.

For the reasons set forth above, it is respectfully submitted that all of the pending claims are now in condition for allowance. Therefore, the issuance of a formal Notice of Allowance is believed next in order, and that action is most earnestly solicited.

To the extent necessary to make this reply timely filed, the Applicant petitions for an extension of time under 37 C.F.R. § 1.136.

If any applicable fee is missing or insufficient, throughout the pendency of this application, the Commissioner is hereby authorized to any applicable fees and to credit any overpayments to our Deposit Account No. 50-1302.

Respectfully submitted,
HICKMAN PALERMO TRUONG & BECKER LLP



Craig G. Holmes
Reg. No. 44,770

Date: July 6, 2004

1600 Willow Street
San Jose, CA 95125
Telephone: (408) 414-1080, ext. 207
Facsimile: (408) 414-1076

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Hon. Commissioner for Patents, Mail Stop AMENDMENT, P.O. Box 1450, Alexandria, VA 22313-1450.

on 7/6/04 by